НОВАЯ ГАЗЕТА

КОММЕНТАРИЙ • ОБЩЕСТВО

Ломают все

Уязвимость интернета компенсируется расходами на компьютерную безопасность. Там, где есть деньги и где власть не главный взломщик

Фото: Евгений Павленко / Коммерсантъ

15:37, 6 августа 2025,

Антон Меркуров

Взлом авиакомпании «Аэрофлот» в очередной раз показал уязвимость критической инфраструктуры в период импортозамещения. Есть версия, что именно переход на российский софт создал целый зоопарк плохо связанных между собой сервисов, что привело к появлению большого количества уязвимостей. И это не единственное событие. Каждый день что-то падает, утекают миллионы персональных данных. Или просто отключают связь. Складывается впечатление, что интернет стал чаще ломаться. Так ли это и что стоит за этими поломками?

За примерами долго ходить не надо, новостей было достаточно. Вот, например, утечки данных в России: Black Star Wear, «ПиццаСушиВок», «Детский мир». И это только самые яркие и известные компании. Еще в прошлом году Россия стала лидером по количеству утечек персональных данных. Никаких причин, что рейтинг изменится в этом году, нет. Хоть где-то — впереди планеты всей.

Под прицелом — и государство. Пожалуй, самый яркий скандал — взлом Росреестра. Последствия утечки будут выражаться в постоянных журналистских расследованиях. Тяжело приходилось МИДу и Роскомнадзору — ведомства находятся на рубежах схватки и логично получают первыми. Не забыт и взлом ВГТРК — государственную телекомпанию вполне можно отнести к органам власти.

В реальности масштабы трагедии больше. Страдают все, так что примеры на этом не заканчиваются. «Билайн», ЛАНИТ — один из крупнейших в стране системных интеграторов. «Лукойл». И это только то, что хорошо прогремело в новостях. Сколько атак осталось незамеченными — хороший вопрос. И это все на фоне отключений и инфраструктурных аварий.

И так — каждый день. В реальности — каждую секунду. Трафик,

задача которого — вывести из строя те или иные системы, несется через разнообразные сети. Главная кибервойна — между США и Китаем. Но в текущих масштабах это ничего не значит. Чтобы оценить масштабы трагедии, прекрасно подходит карта кибератак от компании Check Point. Она помогает понять — это не только российская проблема.

Утечки данных — Adidas, Ticketmaster, страховая компания Allianz. Госорганы США пострадали от уязвимости в Microsoft SharePoint. Да и падало все не только из-за хакеров или желания конкретных ведомств: прошлым летом из-за неудачного обновления Microsoft Windows случилась крупнейшая информационная катастрофа с ущербом в миллиарды. Все перечисленное — только за последний год. Дальше — больше.

Можно констатировать: виртуальная жизнь стала, мягко говоря, насыщеннее за последние годы. Как в инфраструктурной ее части — какой-нибудь спутниковый интернет Starlink или робот от Boston Dynamics — уже привычные явления, так и в области приложений. Достаточно произнести волшебное «искусственный интеллект» — и дальше можно не продолжать. Движение к ноосфере набирает скорость.

Фото: Михаил Метцель / ТАСС

> Киберпреступность, атаки, взломы и прочие неприятные вещи растут соответствующими темпами. Как и цена человеческих ошибок.

Как в случае с программистом из компании CrowdStrike, по чьей вине произошел тот самый прошлогодний сбой с Windows.

Если не погружаться в подробности, в том числе и для того, чтобы не позориться перед настоящими специалистами по информационной безопасности, то происходящее можно разделить на группы:

- **Фоновая преступность**

Чтобы стать жертвой киберпреступника, достаточно просто

что-то сделать в интернете. Попробуйте сайт открыть. Любой. К вам тут же будет лететь какой-то спам. А если вы — какой-то реальный бизнес, это уже не просто спам, а большие атаки. Которые, впрочем, компенсируются расходами на безопасность. Удивительно, но тут ничего личного. Есть дверь — на всякий случай надо пнуть ногой, а вдруг откроется. В интернете ты можешь тысячи таких дверей пинать.

- **Бизнес-разборки**

Положить IT-инфраструктуру конкурента, предаться радостям промышленного шпионажа, просто нагадить, в конце концов. Обычно это дорогое развлечение для взрослых.

- **Киберполитика**

Все страны, где есть интернет, воюют между собой. Без исключения. Все ведомства ежеминутно переживают атаки: желающих украсть ценные документы или просто вывести из строя какое-нибудь государственное учреждение — очередь стоит. Понятно, что на краю Европы своя история. Легендарные «русские хакеры», подразделения, условно говоря, СВР или группы, работающие в интересах ФСБ. Против них — «Кибер Партизаны», белорусское объединение, взявшее на себя ответственность за последнюю атаку на «Аэрофлот».

- **Человеческий фактор**

«Меня взломали» — лучшая отмазка за вчерашнее неподобающее поведение. Но иногда те или иные виртуальные инциденты — дело рук человеческих. Кофе пролили на клавиатуру — бывает. Но признавать не хочется. Причины аварий, утечек и прочих виртуальных инцидентов вполне могут быть прозаичны. В России, например, иногда специально интернет отключают. Всякое в мире бывает. Тут уж вариантов может быть масса.

Как страшно жить в этих ваших интернетах. Во всяком случае, так может показаться на первый взгляд. Бесконечные DDoS-атаки, кажется, непобедимый фишинг. Нет-нет, да попадется в почте письмо, практически неотличимое от оригинала. Хакеры — при поддержке правительства. Уязвимости самих устройств. Утечки данных. И главное — наша тотальная зависимость от всего этого дела. Жизнь без сети кажется уже невозможной.

Но если исключить политику, то киберпреступность и, соответственно, ее сестра, кибербезопасность давно стали рутинными процессами. Это большая индустрия, которая теперь, с началом распространения искусственного интеллекта, решает новые проблемы. Например, Cloudflare, которая помогает, в том числе, и от атак защищаться, теперь с ИИ-ботами сражается. Все выходит на новый уровень. И требует новых решений.

По большому счету, решение большинства проблем — это вопрос инвестиций в информационную безопасность. А остальные — неизбежны. Живут же где-то люди спокойно.

> Но в российском суверенном интернете — свои местные проблемы. Санкции. Железо подорожало, ввозить тяжелее, свое — это на китайском наклейку поменяли. Импортозамещение софта — иллюзия.

Переход «Аэрофлота» с SAP на 1С — мученичество со своими последствиями. Результатами утечек будем еще долго наслаждаться.

Общая экономическая ситуация: чтобы взламывали и ничего не падало — надо постоянно деньги тратить. А тут и так

айтишников не хватает — настолько, что уехавших за любые коврижки умоляют вернуться. Выучить новых — тоже деньги. А их нет. Ну и так далее, что уж тут причитать — и так все всё понимают. Если в реальном мире происходит какая-то дичь, то это непременно отражается и на виртуальном пространстве.

Ущерб оценить сложно, но в случае того же «Аэрофлота» речь идет о десятках миллионов долларов. Плюс — долгие политические последствия. Такова цена прогресса в конкретной ситуации. Если общую деградацию российской IT-инфраструктуры помножить на текущую ситуацию, то можно сделать логичный вывод: будет хуже, суверенный интернет, может, и скрепный, но очень уязвимый. Вчера ВГТРК, сегодня «Аэрофлот». Кто завтра?

ЧИТАЙТЕ ТАКЖЕ:

«У российских и украинских хакеров одна школа — очень хорошая»

Кто и почему «уронил» «Аэрофлот»

16:54, 28 июля 2025, Ирек Муртазин